CLAIMS

What is claimed is:

1. A method for tokenless biometric authorization of an electronic communication, using a biometric sample, a master electronic identicator, and a public communications network, wherein said method comprises:

   a. an electronic communication formation step, wherein at least one communication comprising electronic data is formed;

   b. a user registration step, wherein a user electronically submits a registration biometric sample taken directly from the person of the user;

   c. a public network data transmittal step, wherein the registration biometric sample is electronically transmitted to a master electronic identicator via a public communications network, said master electronic identicator comprising a computer database which electronically stores all of the registration biometric samples from all of the registered users;

   d. a user registration biometric storage step, wherein the registration biometric sample is electronically stored within the master electronic identicator;

   e. a bid biometric transmittal step, wherein a bid biometric sample, taken directly from the person of the user, is electronically transmitted to at least one electronic identicator;

   f. a user identification step, wherein an electronic identicator compares the bid biometric sample to at least one registration biometric sample previously stored in an electronic identicator, for producing either a successful or failed identification of the user;

   g. an electronic communication authorization step, wherein upon a successful identification of the user by an electronic identicator, at least one electronic communication is authorized for execution;

wherein an electronic communication is biometrically-authorized without the user having to present any personalized man-made memory tokens such as smartcards, or magnetic stripe cards.

2. The method of claim 1 wherein during the bid biometric transmittal step, the electronic identicator comprises any of the following: a master electronic identicator, and; a subset electronic identicator, said subset electronic identicator comprising a computer database which electronically stores a subset of all of the registration biometric samples from registered users.

3. The method of claim 1 wherein any steps of said method occur in any of the following chronological sequences: simultaneously, and; separated by any increment of time including seconds, minutes, hours, days, weeks, months, and years.

4. The method of claim 1, further comprising:

   a. a first comparison step, wherein a subset electronic identicator compares the bid biometric sample taken directly from the person of the user with at least one registration biometric sample previously stored in the subset electronic identicator for producing either a successful or failed identification of the user;

   b. a public network data transmittal step, wherein if the subset electronic identicator returns a failed identification result, the bid biometric sample is electronically transmitted via a public communications network to a master electronic identicator;

   c. a second comparison step, wherein a master electronic identicator compares the bid biometric sample to at least one registration biometric sample previously stored in the master electronic identicator for producing either a successful or failed identification of the user;

   d. a communication authorization step, wherein upon the earliest successful identification of the user by an electronic identicator, at least one electronic communication is authorized for execution;

wherein an electronic communication is biometrically-authorized without the user having to present any personalized man-made memory tokens such as smartcards, or magnetic swipe cards.

5. The method of claim 1 further comprising:

   a. an enterprise registration step, wherein an enterprise electronically submits registration identity data;

b. a public network data transmittal step, wherein the enterprise registration identity data is electronically transmitted to a master electronic identicator via a public communications network;

c. an enterprise registration identity data storage step, wherein the enterprise registration identity data is electronically stored within the master electronic identicator;

d. an enterprise bid identity data network transmittal step, wherein enterprise bid identity data is electronically transmitted to at least one electronic identicator, said electronic identicator comprising any of the following: a subset electronic identicator and a master electronic identicator;

e. an enterprise identification step, wherein an electronic identicator compares the enterprise bid identity data with enterprise registration identity data previously stored in the electronic identicator, for producing either a successful or failed identification of the enterprise;

f. an electronic communication authorization step, wherein upon a successful identification of the enterprise by an electronic identicator and a successful identification of the user by an electronic identicator, at least one electronic communication is authorized for execution;

wherein an electronic communication is biometrically-authorized without the user having to present any personalized man-made memory tokens such as smartcards, or magnetic swipe cards.

6. The method of claim 5 wherein any steps of said method occur in any of the following chronologies: simultaneously, and; separated by any increment of time including seconds, minutes, hours, days, weeks, months, and years.

7. The method of claim 5 further comprising:

a. a first comparison step, wherein a subset electronic identicator compares the enterprise bid identity data with enterprise registration identity data previously stored in the subset electronic identicator for producing either a successful or failed identification of the enterprise;

b. a public network data transmittal step, wherein if the subset electronic identicator returns a failed identification result, the enterprise bid identity data is electronically transmitted via a public communications network to a master electronic identicator;

c. a second comparison step, wherein a master electronic identicator compares the enterprise bid identity data with enterprise registration identity data previously stored in the master electronic identicator for producing either a successful or failed identification of the enterprise;

d. a communication authorization step, wherein upon the earliest successful identification of the user by an electronic identicator and the earliest successful identication of the enterprise by an electronic identicator, at least one electronic communication is authorized for execution;

wherein an electronic communication is biometrically-authorized without the user having to present any personalized man-made memory tokens such as smartcards, or magnetic swipe cards.

8. The method of claim 1 wherein the biometric sample taken directly from the person of the user comprises any of the following: a fingerprint, a facial scan, a retinal image, an iris scan, and a voice print.

9. The method of claim 5 wherein the enterprise is a legally formed entity comprising any of the following: a corporation, a foundation, a non-profit organization, a sole proprietorship, a limited liability company, and a partnership.

10. The method of claim 1 wherein during the user identification step, the user provides a personal identification code to the electronic identicator along with a bid biometric sample for purposes of identifying the user.

11. The method of claim 1 further comprising a user re-registration check step, wherein the user's registration biometric sample is compared by at least one electronic identicator to previously registered biometric samples wherein if a match occurs, the electronic identicator is alerted to the fact that the user has attempted to re-register.

12. The method of claim 10 further comprising a biometric theft resolution step, wherein a user's personal identification code is changed when the user's registered biometric sample is determined to have been fraudulently duplicated.

13. The method of claim 1, wherein an electronic communication comprises any of the following: an email communication, a telephone call, an encrypted data packet, an Internet telephony communication, and a facsimile.

14. The method of claim 1, wherein during the communication authorization step, any of the following is used: an intranet, an extranet, a local area network, a wide area network, a cable network, a wireless network, a telephone network, the Internet, an ATM network, or an X.25.

15. The method of claim 5 wherein enterprise registration identity data comprises any of the following: an alpha-numeric code, a hardware identification code, an email address, a financial account, a biometric of an authorized enterprise representative, a non-financial data repository account, a telephone number, a mailing address, a digital certificate, a network credential, an Internet protocol address, a digital signature, an encryption key, and an instant messaging address.

16. The method of claim 1 wherein the communication authorization step further comprises a third-party communications step, wherein the electronic identicator electronically communicates with a third-party server in order to authorize the electronic communication.

17. The method of claim 1 further comprising:

    a. a rule-module formation step, wherein a rule-module is formed in an electronic clearinghouse, said rule-module further comprising at least one user-customized pattern data which is associated with at least one execution command;

    b. a rule-module invocation step, wherein upon a successful identification of the user, at least one previously designated user-customized rule-module is invoked;

    c. an electronic communication execution step, wherein upon the invocation of a user-customized rule-module, at least one electronic communication is executed.

18. The method of claim 17 wherein pattern data comprises any of the following: a user unique identification code; demographic information; an email address; a financial

account; a biometric; internet browsing patterns; a non-financial data repository account; a telephone number; a mailing address; purchasing patterns; database authorization fields; financial credit report data; a call-center queuing, routing and automated response program; an email-center queuing, routing and automated response program; data on pre-paid accounts or memberships for products or services; electronic data utilization patterns; employee status; job title; data on user behavior patterns; a digital certificate; a network credential; an internet protocol address; a digital signature; an encryption key; an instant messaging address; user-customized medical records; an electronic audio signature; and an electronic visual signature.

19. The method of claim 17 wherein said execution commands further comprise user-customized instructions for executing any of the following: accessing of stored electronic data, processing of electronic data, and presentation of electronic data.

20. The method of claim 19 wherein user-customized accessing of stored electronic data further comprises execution of any of the following: activating of an Internet-connected device; accessing of a secured physical space, and unlocking of a secured physical device.

21. The method of claim 19, wherein user-customized processing of electronic data further comprises invoking any of the following: a digital certificate, an identity scrambler, a database authorization field, an electronic consumer loyalty or consumer rewards incentive, an electronic advertisement, an instant messaging program, real-time tracking of an incoming caller or an email sender, a time and attendance monitoring program, an emergency home alarm and personal safety notification program, a real-time challenge-response program, a call-center queuing prioritization program, a call-center routing prioritization program, an email-center queuing prioritization program, an email-center routing prioritization program, an automated caller or emailer response program, a call-forwarding program, and an electronic intelligent software program for electronic data search and retrieval.

22. The method of claim 19 wherein user-customized presentation of electronic data comprises any of the following: a print-out, a computer screen display, an audio message, a tactile sensation and a holographic image.

23. The method of claim 17 wherein the rule-module invocation step further comprises a third-party communications step, wherein the electronic rule-module clearinghouse communicates with one or more third-party computers in order to invoke a rule-module.

24. The method of claim 17, wherein user-customized pattern data is provided to the electronic rule-module clearinghouse by any of the following: the user, the electronic identicator, the electronic rule-module clearinghouse, and a user-authorized third party.

25. The method of claim 17, wherein user-customized execution commands are provided to the electronic rule-module clearinghouse by any of the following: the user, the electronic rule-module clearinghouse, the electronic identicator and a user-authorized third party.

26. The method of claim 17 further comprising:

a. a master rule-module storage step, wherein all of the rule-modules from all of the registered users are stored in a master rule-module clearinghouse ;

b. a subset rule-module storage step, wherein a subset of all of the rule-modules from registered users is stored in a subset rule-module clearinghouse;

c. a rule-module invocation step, wherein upon a successful identification of the user, at least one user-customized rule-module is invoked by any of the following: a subset rule-module clearinghouse and a master rule-module clearinghouse;

d. an electronic communication execution step, wherein upon the invocation of a user-customized rule-module, at least one electronic communication is executed.

27. The method of claim 1 wherein during the registration biometric network transmittal step, any of the following public networks is used: a cable network, a wireless cellular network, a wireless digital network, a telephone network, a wide area network, the Internet, an ATM network, and an X.25 connection.

28. The method of claim 1 wherein during the public network data transmittal step, any of the following networks is used: a cable network, a wireless cellular network, a

wireless digital network, a telephone network, a wide area network, the Internet, an ATM network, and an X.25 connection.

29. The method of claim 26 further comprising:
    a. a first rule-module invocation step, wherein the subset rule-module clearinghouse attempts to invoke at least one user-customized rule-module;
    b. a public network data transmittal step, wherein if the subset rule-module clearinghouse fails to invoke a user-customized rule-module, the request is transmitted to a master rule-module clearinghouse via a public communications network;
    c. a second rule-module invocation step, wherein a master rule-module clearinghouse attempts to invoke at least one user-customized rule-module;
    d. an electronic communication execution step, wherein upon the earliest invocation of a user-customized rule-module, at least one electronic communication is executed.
30. The method of claim 26 wherein the master rule-module clearinghouse comprises a computer database which electronically stores all of the rule-modules for all of the registered users.
31. The method of claim 26 wherein the subset rule-module clearinghouse comprising a computer database which electronically stores a subset of all of the rule-modules for registered users.

32. A system for tokenless biometric authorization of an electronic communication, using an electronic communication input apparatus, a biometric input apparatus, and a master electronic identicator, wherein said system comprises:
    a. a communication input apparatus, further comprising a data entry device for formation of an electronic communication;
    b. a biometric input apparatus, further comprising a device for electronically scanning a biometric sample directly from the person of a user;
    c. at least one master electronic identicator, further comprising:
        i) a computer database containing all of the electronically stored biometric samples from all of the registered users;

ii) a comparator that electronically compares received a biometric sample with previously stored biometric samples to deliver either a successful or failed identification of the user;

d. a data transmittal public network that electronically transmits data between the biometric input apparatus and a master electronic identicator;

e. an electronic communication authorization platform that authorizes execution of at least one electronic communication upon a successful identification of the user by an electronic identicator;

wherein an electronic communication is biometrically-authorized without the user having to present any personalized man-made memory tokens such as smartcards, or magnetic stripe cards.

33. The device of claim 32 wherein the master electronic identicator further comprises a computer database which: has a location which is physically remote from the site at which the user submits a biometric sample directly from his person, and; requires the use of a public communication network that enables receipt of an electronically transmitted registration biometric sample.

34. The device of claim 32 further comprising a subset electronic identicator having: a computer database containing a subset of all stored biometric samples from registered users in the computer system, and; a comparator that compares a received biometric sample with previously stored biometric samples to deliver either a successful or failed identification of the user.

35. The device of claim 32 wherein any component of said system is used in any of the following chronological sequences: simultaneously, and; separated by any increment of time including seconds, minutes, hours, days, weeks, months, and years.

36. The device of claim 34, further comprising:

a. a first comparator, comprising a subset electronic identicator comparator that compares the bid biometric sample taken directly from the person of the user with at least one registration biometric sample previously stored in the subset electronic identicator for producing either a successful or failed identification of the user;

b. a data transmittal public network, comprising a public communications network that electronically electronically transmits data between the subset electronic identicator and a master electronic identicator;

c. a second comparator, comprising a master electronic identicator comparator which, if the subset electronic identicator fails to successfully identify the user, compares the bid biometric sample to at least one registration biometric sample previously stored in the master electronic identicator for producing either a successful or failed identification of the user;

d. a communication authorization platform, that authorizes execution of an electronic communication upon the earliest successful identification of the user by an electronic identicator;

wherein an electronic communication is biometrically-authorized without the user having to present any personalized man-made memory tokens such as smartcards, or magnetic swipe cards.

37. The device of claim 34 further comprising:

a. an enterprise data input apparatus for an enterprise to electronically input registration identity data;

b. a data transmittal public network, further comprising a public communications network that electronically transmits data between the enterprise data input apparatus and a master electronic identicator;

c. an electronic communication authorization platform, that authorizes execution of an electronic communication upon a successful identification of the enterprise by an electronic identicator and a successful identication of the user by an electronic identicator;

wherein an electronic communication is biometrically-authorized without the user having to present any personalized man-made memory tokens such as smartcards, or magnetic swipe cards.

38. The device of claim 37 wherein any component is used in any of the following chronological sequences: simultaneously, and; separated by any increment of time including seconds, minutes, hours, days, weeks, months, and years.

39. The device of claim 37 further comprising:

a. a first comparator, comprising a subset electronic identicator comparator that compares the enterprise bid identity data with enterprise registration identity data previously stored in the subset electronic identicator for producing either a successful or failed identification of the enterprise;

b. a data transmittal public network, further comprising a public communications network that electronically transmits data between the subset electronic identicator and a master electronic identicator;

c. a second comparator, comprising a master electronic identicator comparator which, if the subset electronic identicator fails to successfully identify the enterprise, compares the enterprise bid identity data with enterprise registration identity data previously stored in the master electronic identicator for producing either a successful or failed identification of the enterprise;

d. a communication authorization platform, that authorizes execution of an electronic upon the earliest successful identification of the user by an electronic identicator and the earliest identification of the enterprise by an electronic identicator;

wherein an electronic communication is biometrically-authorized without the user having to present any personalized man-made memory tokens such as smartcards, or magnetic swipe cards.

40. The device of claim 32 wherein the biometric sample taken directly from the person of the user comprises any of the following: a fingerprint, a facial scan, a retinal image, an iris scan, and a voice print.

41. The device of claim 37 wherein the enterprise is a legally formed entity comprising any of the following: a corporation, a foundation, a non-profit organization, a sole proprietorship, a limited liability company, and a partnership.

42. The device of claim 32 wherein the user further provides a personal identification code to the electronic identicator along with a bid biometric sample for purposes of identifying the user.

43. The device of claim 37 further comprising a user re-registration platform, wherein the user's registration biometric sample is compared by at least one electronic identicator to previously registered biometric samples wherein if a match occurs, the electronic identicator is alerted to the fact that the user has attempted to re-register.

44. The device of claim 42 further comprising a biometric theft resolution platform, wherein a user's personal identification code is changed when the user's registered biometric sample is determined to have been fraudulently duplicated.

45. The device of claim 32, wherein an electronic communication comprises any of the following: an email, a telephone call, an encrypted data packet, an Internet telephony, and a facsimile.

46. The device of claim 32, wherein the data transmittal public network further comprises any of the following: an extranet, a wide area network, a cable network, a wireless network, a telephone network, the Internet, an ATM network, or an X.25.

47. The device of claim 37 wherein enterprise registration identity data comprises any of the following: an alpha-numeric code, a hardware identification code, an email address, a financial account, a biometric of an authorized enterprise representative, a non-financial data repository account, a telephone number, a mailing address, a digital certificate, a network credential, an Internet protocol address, a digital signature, an encryption key, and an instant messaging address.

48. The device of claim 32 further comprising a third-party server interconnecting network, wherein the electronic communication execution platform interconnects with one or more third-party servers in order to execute the electronic communication.

49. The device of claim 32 further comprising:

a. a rule-module clearinghouse, further comprising at least one user-customized pattern data which is associated with at least one execution command;

b. a rule-module invocation platform, that invokes at least one previously designated user-customized rule-module upon successful identification of the user;

c. an electronic communication execution platform, that executes at least one electronic communication upon the invocation of a user-customized rule-module.

50. The device of claim 49 wherein pattern data comprises any of the following: a user unique identification code: demographic information; an email address; a financial account; a biometric; internet browsing patterns; a non-financial data repository account; a telephone number; a mailing address; purchasing patterns; database authorization fields; financial credit report data; a call-center queuing, routing and automated response program; an email-center queuing, routing and automated response program; data on pre-paid accounts or memberships for products or services; electronic data utilization patterns; employee status; job title; data on user behavior patterns; a digital certificate; a network credential; an internet protocol address; a digital signature; an encryption key; an instant messaging address; user-customized medical records; an electronic audio signature; and an electronic visual signature.

51. The device of claim 49 wherein said execution commands further comprise user-customized instructions for execution of any of the following: accessing of stored electronic data, processing of electronic data, and presentation of electronic data.

52. The device of claim 51 wherein user-customized accessing of stored electronic data further comprises execution of any of the following: activation of an Internet-connected device; accessing of a secured physical space, and unlocking of a secured physical device.

53. The device of claim 51, wherein user-customized processing of electronic data further comprises invoking any of the following: a digital certificate, an identity scrambler, a database authorization field, an electronic consumer loyalty or consumer rewards incentive, an electronic advertisement, an instant messaging program, real-time tracking of an incoming caller or an email sender, a time and attendance monitoring program, an emergency home alarm and personal safety notification program, a real-time challenge-response program, a call-center queuing prioritization program, a call-center routing prioritization program, an email-center queuing prioritization program, an email-center routing prioritization program, an automated caller or emailer

response program, a call-forwarding program, and an electronic intelligent software program for electronic data search and retrieval.

54. The device of claim 51 wherein user-customized presentation of electronic data comprises any of the following: a print-out, a computer screen display, an audio message, a tactile sensation and a holographic image.

55. The device of claim 49 wherein the rule-module invocation platform is interconnected with one or more third-party computers.

56. The device of claim 49, wherein user-customized pattern data is provided to the electronic rule-module clearinghouse by any of the following: the user, the electronic identicator, the electronic rule-module clearinghouse, and a user-authorized third party.

57. The device of claim 49, wherein user-customized execution commands are provided to the electronic rule-module clearinghouse by any of the following: the user, the electronic rule-module clearinghouse, the electronic identicator and a user-authorized third party.

58. The device of claim 49 further comprising:

a. a master rule-module clearinghouse, comprising a computer database storing all of the rule-modules for all of the registered users;

b. a subset rule-module clearinghouse, comprising computer database storing a subset of all of the rule-modules for registered users;

c. a rule-module invocation platform, that invokes at least one user-customized rule-module upon identification of the user, said platform comprising any of the following: a subset rule-module clearinghouse and a master rule-module clearinghouse;

d. an electronic communication execution platform, that executes at least one electronic communication upon the invocation of a user-customized rule-module.

59. The device of claim 32 wherein the data transmittal public network further comprises: a cable network, a wireless cellular network, a wireless digital network, a telephone

network, a wide area network, the Internet, an ATM network, and an X.25 connection.

58. The device of claim 32 wherein the master electronic identicator further comprises a computer database having a location which is physically remote from the site at which the user submitted the registration biometric sample.

60. The device of claim 34 wherein the subset electronic identicator further comprises a computer database: being physically remote from the master identicator, and; capable of using any communications network for receiving the bid biometric sample.

61. The device of claim 58 further comprising:

a. a first rule-module invocation platform, comprising a subset rule-module clearinghouse that invokes at least one user-customized rule-module;

b. a data transmittal public network, wherein if the subset rule-module clearinghouse fails to invoke a user-customized rule-module, the request is transmitted via a public communications network to a master rule-module clearinghouse;

c. a second rule-module invocation platform, comprising a master rule-module clearinghouse that invokes at least one user-customized rule-module;

d. an electronic communication execution platform, that executes at least one electronic communication upon the earliest invocation of a user-customized rule-module by a rule-module clearinghouse.

62. The device of claim 58 wherein the subset rule-module clearinghouse is physically remote from the master rule-module clearinghouse.